

Cryptocurrencies: The Dawn of a New Age

Piyush Thukral*

ABSTRACT

Cryptocurrencies have gained relevance in today's economic forum with the advent of technology and computing. Cryptocurrencies are a form of decentralized digital currency which has created a niche of investors all around the globe. The cryptographic forms of money have shown bounteous development and capital appreciation that has additionally charmed the financial specialists in the worldwide standpoint. This paper makes an endeavor to clarify what Cryptocurrencies are. It likewise tries to summon the advantages and disadvantages of the Cryptocurrencies and give some understanding into the street ahead for the Cryptocurrencies in India.

Keywords- Cryptocurrencies, Bitcoins, Digital Currency

* Assistant Audit Officer, Indian Audit & Accounts Department,
E-mail: pt.4132@gmail.com

INTRODUCTION

The recent splurge in the crypto currency showcase has made it important to make people comprehend what crypto currency implies. A key meaning of crypto currency is that it is a type of digital currency that is decentralized and utilizes cryptography for auxiliary security, making it tough to counterfeit, manipulate or control.

Basically, Cryptocurrencies are innovative virtual payments frameworks that don't depend on a principal authority to produce currency supply or to confirm, track, and record transactions. They most nearly take after a **fiat** currency that isn't supported by a Central Bank and that has a stable, predefined rate of currency supply growth. Cryptocurrencies are so called based on the grounds that cryptographic methods lie at the core of their usage. A crypto currency demonstrates the following traits:

1. No physical existence and just network/digital existence.
2. No intrinsic value.
3. Its source of supply is neither controlled nor **dictated** by the central bank.

Different Cryptocurrencies can be found in the current financial foray since the appearance of Bit coin in 2009. Lit coin, Ether, Ripple, Dash, and Doge coin are some of the popular Cryptocurrencies in the current financial expedition apart from Bit coin.

OBJECTIVES

The examination is a way to satisfy the following targets:

1. To give a brief depiction of what Cryptocurrencies are and how they function.
2. To contribute a familiarity into the upsides and downsides of Cryptocurrencies.
3. To give a short portrayal of the prominence of cryptocurrencies in the Indian state of affairs.

RESEARCH METHODOLOGY

This is a theoretically organized examination and thus, theory and testing can't be related. In that limit, the views imparted in this paper are the author's

own specific deductions and the assessments of certain reputed authors.

FINDINGS AND DISCUSSION

With a specific end goal to provide a better and simple conception of what it is and how it functions, some crypto currency jargon requires understanding:

- **Block chain** –The crypto currency exchanges are recorded chronologically and publicly through a decentralized and computerized ledger, known as block chain in **crypto currency** terminology. The block contains data that once go into the block chain turns out to be a piece of the lasting and permanent database, interfacing with different blocks in the block chain.
- **Block**–A block alludes to an aggregation of data related to transactions that are packaged together with a preordained size. They are administered for transactional authentication and in the long run turn into a bit of a block chain.
- **Mining** – Mining is the term utilized for discerning and deciphering blocks along the block chain. An incentive is given for unraveling the algorithm and prolonging the chain, called a mining reward. **The mining reward for the Bit coin block chain is Bit coin.**
- **Proof of Work** – The process of updating the ledger is made difficult purposefully by making satisfaction of specific requirements obligatory and this result into a fragment of data, which was termed as the “proof-of-work”. The generation of a proof of work is an unpredictable approach with low probability, so it requires a huge amount of experimentation before a substantial “proof-of-work” is made. This difficulty serves two purposes: it confines the degree of crypto currency creation and it bolsters the integrity of the currency by making it troublesome, for a node to affix and keep up deceitful transactions in the block chain.
- **P2P** – It stands for Peer-to-Peer. P2P has turned into an all-embracing focus of block chain as one of the paramount marketing points of crypto currency is decentralization. Practically every association on the block chains fulfilled P2P, or without a centralizing variable like a bank.

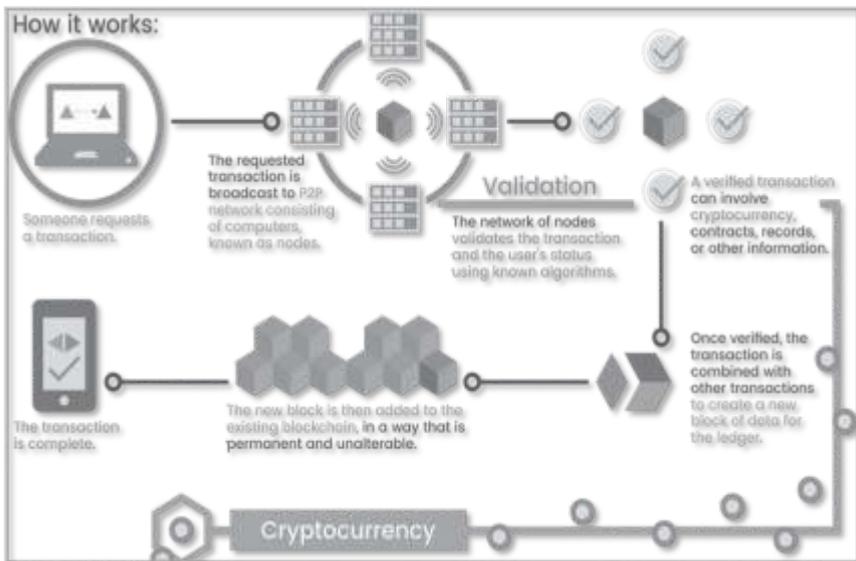
- **Node** – A Node is basically a computer associated with the P2P network. A node strengthens the framework through authentication as well as relaying of transactions whilst accepting a replica of the entire block chain itself.
- **Fiat money** – It alludes to the currencies that have insignificant or no inherent worth themselves but rather are characterized as legitimate currency by the government, for example, paper bills and coins. The supply of these fiat currencies is controlled by the central banks of respective nations. These central banks also shoulder the responsibility of adding anti-counterfeiting features to physical currency bills and coins. These security highlights increase current standards for an assailant; however, they don't prove difficult to fake. At last, law implementation is vital for preventing individuals from breaking the tenets of the framework.
- **Address** – An address is a protected identifier discernable by a distinctive string of characters that empowers payments to an individual or entity by means of block chain transactions. An address is generally accompanied by a private key to gain exclusive access to the funds. For example, Bit coin addresses are alphanumeric strings that begin with a 1 or 3; Ethereum addresses tend to start with '0x'.
- **Distributed Ledger** – A dispersed or distributed ledger is an arrangement of mutual, replicable and synchronized information spread over various computer systems. In the event of Cryptocurrencies, rather than the data dwelling on a solitary concentrated server, it is replicated crosswise over a huge number of nodes around the world, consequently loaning it a decentralized nature

Having experienced some technical terms identified with crypto currency, the inquiry that emerges is the manner in which these technicalities work in tandem to satisfy a transaction on the crypto-currency network.

A basic outline of this procedure would give one better understanding of how the crypto currency transaction occurs. Let us begin with a basic presumption that some individual wants to make a transaction in crypto currency. The requested transaction is then publicized to the P2P network which comprises of nodes. After this, a network of nodes validates the transaction by means of algorithms. Once verified, the transaction is

combined with other transactions giving rise to a new block of data. The new block created, is then added to the existing block chain/digital ledger making it permanent and unalterable part of a large database. Once the mining is done, a proof of work is generated that renders the transaction complete.

Figure 1: Modus operandi of Crypto currency



(Source:<https://blockgeeks.com/guides/what-is-cryptocurrency/#>)

Shortcomings of Crypto currency

Distrusted

Crypto currency is not yet as widely known as they need to be. Since only a small niche of people is aware of it and even a smaller subset of that niche understands how it works, people tend to be mistrustful of Cryptocurrencies. Consequently, the number of organizations that accept crypto currency as a medium of exchange is very few as of now. This is a constraint for the general masses that wish to utilize crypto currency for their daily transactions.

Irretrievable

Unlike the fiat currencies which are controlled by central banks, Cryptocurrencies are decentralized. The security issues concerning the fiat currencies are handled by these central banks, whereas Cryptocurrencies once lost cannot be recovered due to the absence of centralized authority. Another cause contributing to this drawback is the fact that the cryptocurrencies are encrypted for security purposes. The encryption distinguishes the currency, but not the owner. Whoever has the codes owns the crypto currency and this anonymity feature thus, makes sure that crypto currency once stolen is lost forever.

Pseudonymous transactions

This element makes crypto currency the ideal device for criminal transactions. Much the same as drug dealers and other crooked individuals utilize cash to maintain a strategic distance from discovery; transactions made with Cryptocurrencies are practically untraceable. This could be the motivation behind why a few governments have announced Cryptocurrencies such as Bit coin illicit medium of exchange in their nations.

High Volatility

What people often neglect due to the technicalities involved with Cryptocurrencies is the way in which the value/prices of Cryptocurrencies are subject to market fluctuations just like gold, oil, and some other commodities. The prices or exchange value of Cryptocurrencies exhibit high degree of volatility and as such may be deemed as a high risk and unseemly speculation by some economists.

The value of Cryptocurrencies is as yet unstable, with unexpected rapid rises and sudden plunges. This instability may be illustrated by the trend chart represented below. The trend chart represents the volatility in the value of Bit coin on December 6, 2017, from midnight to noon. The profoundly unstable nature can be effortlessly followed and gaged through the countless peaks and valleys in the trend line.

Figure 2: BitCoin (USD) Price (December 6, 2017)



(Source: <https://www.coindesk.com/price>)

Perpetual Loss of Access

Loss or theft of key required to access one's account may bring about the perpetual loss of access for the owner of the crypto currency. It is in fact nearly impossible to reestablish access to the existing crypto currency account if the key is lost or stolen, because of the perpetual utilization of cryptographic systems.

Irreversible transaction

A transaction once recorded in a block chain winds up plainly unalterable and eternal. This suggests that the customer himself is responsible for any deceitful or mistaken transaction occurring. This may adversely affect the customer security and protection.

51% attack

A 51% attack refers to a scenario where more than half of the processing power on a network is controlled by a solitary individual or a concentrated group, allowing them to influence the entire system. An entity with 51% of the computing power may:

- Issue a transaction that conflicts other transactions.
- Halt authentication of transactions.

- Disburse the same coins numerous times.
- Halt other miners from mining valid blocks.
- Halt and manipulate all interpersonal transactions.

Obstacles by Governments

The crypto currency can't be restricted without prohibiting the internet itself but still, the legislatures of a few nations have prohibited the utilization of crypto currency owing to the looming frauds. It is, in fact, profoundly improbable for the governments being able to distinguish each individual who possesses Cryptocurrencies, but barring them dissuades the business organizations from accepting Cryptocurrencies. Without merchants and organizations willing to acknowledge it, its incentive as a replacement for money becomes negligible.

Strengths of Crypto currency

Transparency

There is an open digital ledger called a block chain on which all transactions are recorded and monitored. Once recorded, the transaction becomes noticeably perpetual and unalterable. This is one of the biggest safety focuses of crypto currency as no individual person, entity or organization can manipulate the transactions, therein creating the transparency.

Inflation is unlikely

Fiat currencies, for the most part, are prone to inflation due to the volatility of prices in the economy and extension of the money supply by governments and central banks. Crypto currency may not encounter this as much on the grounds that there are a finite number of minable crypto currency units. For instance, Bit coin was programmed to have only about 21 million Bit coins. The last of the Bit coins will be created nearby 2050 and after that, no more bit coins will be introduced into the network.

Portability

Distinct from the physical currency, crypto currency can be transferred effortlessly without any likelihood of detection. The portability of crypto currency can be easily comprehended by a simple statement that 'billions of dollars can be stored in the form of Bit coins or Ether on a 'memory drive'.

Control

Since the users of crypto currency are in control of their transactions, this aide in guarding it. Transactions are made autonomous of the identities of the parties making them. This shields the users from identity theft and data fraud.

Pseudonymous

Pseudonymous nature acts as a benefit as well as a hindrance. The lack of detect ability of crypto that no organization can trace the origin of the funds. This entails the freedom to buy and sell Cryptocurrencies without the possibility of the source of funds being traced.

Low transaction charges

As the transactions happen through the block chain over a dispersed P2P network, a third party corroboration and sanction of transactions is not needed. As of now, crypto currency dealings have low charges when compared with customary payment platforms. Be that as it may, this is probably going to change later on based on the incentives that would be offered to the users in order to maintain the network and support development.

Quick transactions

The decentralized idea of crypto currency empowers it to sidestep banks and other financial institutions, and subsequently, the payments and exchanges are finished quickly. This cuts down the time taken to finish the transactions particularly the international ones.

Avoidance of double payment

Since every exchange in the crypto currency framework is recorded by means of the public block chain/digital ledger, the "spending" of the same units of the crypto currency more than once is outlandish. This double payment protection settles the conventional money downside where a clearing middleman is fundamental to the transaction. This is, in any case, based on the premise that the crypto currency ecosystem is sound and isn't penetrated by immoral elements.

Ease of participation

Just like the case is with most digital innovations, utilizing crypto-currency is not an arduous task. All one needs is a computer or a mobile device with internet connectivity in order to set up an account and start transacting in crypto currency.

Crypto currency is an amazing specialized accomplishment, yet it feels as if it is more of a financial experimentation at the moment. Regardless of whether Cryptocurrencies survive and prosper, a look into its upsides and downsides attempts to provide a clear picture as to whether Cryptocurrencies are just a technological phase and a financial bubble that will pass away or whether they are the disruptive finance and technology blend that has the capacity to stand against the fiat currencies in the nearby future.

Crypto currency avenues in India

After witnessing demonetization in 2016, the Indian consumers made a paradigm shift to digital wallets. Paytm and other e-wallets saw a massive splurge in the day to day transactions. It made the masses in India realize the simplicity and the upsides of utilizing the digital means of transactions.

The enormous presence of Cryptocurrencies in the global paraphernalia enamored several Indians who invested in Bit coins amid that period. The crypto currency trading in India has experienced exponential growth in the course of recent months which is going to continue in the days to come.

The spike of Cryptocurrencies did not just infatuate the Indian investor segment but it also sparked certain tech-savvy individuals with the readiness to promote the scope of Cryptocurrencies in India and to innovate on the block chain concept. Laxmi coin and Bit India are a few examples of the innovative and disruptive technologies that are due to hit India in 2018.

With respect to legitimizing crypto currency, the government of India has reiterated its prior perspective of 2013. Through a statement made by the RBI in 2013, the government had made its stance clear by stating that the government neither recognizes nor legitimizes Bit coin or any other crypto currency as a legal tender. RBI cautioned users, holders, and traders of security concerns surrounding Bit coin or any other virtual currencies. In April 2017, the government had constituted a committee to look into crypto

currency legitimacy which had submitted its report in August 2017.

CONCLUSION

With the progressing time and the rapid exponential development of crypto currency trading in the Indian ecosystem, it can be inferred that any further deferral in appropriation and adoption of a crypto currency control and regulation policy would almost make the policy ineffective.

BIBLIOGRAPHY

A Crypto Terminology Guide! A list of all terms Cryptocurrency related. (2017). *Steemit.com*. Retrieved 27 November 2017, from <https://steemit.com/bitcoin/@snapat/jargonit-a-crypto-terminology-guide-a-list-of-all-terms-cryptocurrency-related>

Anupam, S. (2017). *Cryptocurrency This Week: Bitcoin Remains A Pandora's Box For India while Belarus Will Legalise Bitcoins And ICOs.* *Inc42 Media*. Retrieved 3 December 2017, from <https://inc42.com/buzz/cryptocurrency-bitcoin-india-belarus/>

Bitcoin & Cryptocurrency related terminology Flashcards | Quizlet. (2017). *Quizlet.com*. Retrieved 28 November 2017, from <https://quizlet.com/107781909/bitcoin-cryptocurrency-related-terminology-flash-cards/>

Bitcoin (USD) Price. (2017). Retrieved from <https://www.coindesk.com/price/>

Boersma, J., Burgers, G., Huijstee, J., & Rood, M. (2017). *Cryptocurrencies Exploring a revolutionary technology* (pp. 1-51). Innopay. Retrieved from <https://innopay.com/assets/Reports/140623-Innopay-Cryptocurrency-report-0.pdf>

CFA Institute. (2014). *CRYPTO-CURRENCIES Intellectual Curiosity or the Future of Finance?* (pp. 1-9). CFA Institute. Retrieved from <https://www.cfainstitute.org/ethics/Documents/Digital%20Currencies%20Policy%20Brief.pdf>

Chavan, N., & Kapase, S. (2017). Crypto Currency a Need after Demonetization in India. *IJESC*, 7(6), 13599 - 13601. Retrieved from <http://ijesc.org/upload/0fb807c51647eb1fe1e0bf0d34dafbb1.Crypto%20>

Currency%20a%20Need%20after%20Demonetization%20in%20India.pdf

Cryptocurrency. *En.wikipedia.org*. Retrieved 22 November 2017, from <https://en.wikipedia.org/wiki/Cryptocurrency>

Cryptocurrency and Blockchain Glossary A-Z - Crush Crypto. (2017). *Crush Crypto*. Retrieved 27 November 2017, from <https://crushcrypto.com/glossary/>

D'Alfonso, A., Langer, P., & Vandelis, Z. (2016). The Future of Cryptocurrency An Investor's Comparison of Bitcoin and Ethereum. *The Economist*. Retrieved from http://www.economist.com/sites/default/files/the_future_of_cryptocurrency.pdf

DeVries, P. (2016). An Analysis of Cryptocurrency, Bitcoin, and the Future. *International Journal Of Business Management And Commerce*, 1(2), 1 - 9. Retrieved from https://www.researchgate.net/publication/316656878_An_Analysis_of_Cryptocurrency_Bitcoin_and_the_Future

Dourado, E., & Brito, J. (2014). cryptocurrency. *The New Palgrave Dictionary Of Economics Online Edition*. <http://dx.doi.org/10.1057/9780230226203.3924>

Ezugwu, C. *The Pros & Cons Of Cryptocurrency*. *Bizcatalyst360.com*. Retrieved 28 November 2017, from <https://www.bizcatalyst360.com/the-pros-cons-of-cryptocurrency/>

Middelman, M. (2016). *21 Terms to Understand Cryptocurrency – The Mission – Medium*. *Medium*. Retrieved 27 November 2017, from <https://medium.com/the-mission/21-terms-to-understand-cryptocurrency-8bee30aa8dfc>

Mittal, T. (2017). *Bitcoin for beginners: brief overview of the technology*. *YourStory.com*. Retrieved 29 November 2017, from <https://yourstory.com/2017/11/bitcoin-beginners-guide/>

Rosic, A. (2016). *5 Benefits of Cryptocurrency: A New Economy For The Future*. *Decentralize Today*. Retrieved 30 November 2017, from <https://decentralize.today/5-benefits-of-cryptocurrency-a-new-economy-for-the-future-925747434103>

The future of mobile payments in India. (2017). *YourStory.com*. Retrieved 29 November 2017, from <https://yourstory.com/2017/11/future-mobile-payments-india/>

Time to sell your Bitcoins: Cryptocurrencies success a bubble, Central bankers around the world warn. (2017). *The Financial Express*. Retrieved 30 November 2017, from <http://www.financialexpress.com/market/time-to-sell-your-bitcoins-cryptocurrencies-success-a-bubble-central-bankers-around-the-world-warn/949372/>

Vyas, C., & Lunagaria, M. (2014). Security Concerns and Issues for Bitcoin. In *National Conference cum Workshop on Bioinformatics and Computational Biology* (pp. 10 - 12). Sikkim Manipal Institute of Technology: International Journal of Computer Applications. Retrieved from <http://research.ijcaonline.org/ncwbc/number2/ncwbc1414.pdf>

What is Cryptocurrency: Everything You Need To Know [Ultimate Guide]. *Blockgeeks*. Retrieved 30 November 2017, from <https://blockgeeks.com/guides/what-is-cryptocurrency/>